ABSTRACT

A system and method is described in which two parties communicate a first shared random number and a second shared random number, and each independently use a combining function with inputs including the two shared random numbers to obtain a shared secret key. Secure communication of the shared random numbers is performed by using a password and an asymmetric key pair. The password and the private key are not communicated, thereby preventing eavesdroppers from obtaining information sufficient to determine the shared secret key. Direct attacks on the parties are foiled by preventing the password from being stored, not storing the private key, and using two shared random numbers in case one is compromised by an attack on one of the two parties. A party cannot be effectively impersonated without knowledge of the password, and a called party cannot be impersonated without additionally controlling the network.